Data Protection in the Arab Spring

Gayrel, Claire

Published in:
Privacy laws & business international report

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

Data Protection in the Arab Spring: Tunisia and Morocco

Recent political uprisings will be reflected in future changes to the data protection regimes. By **Claire Gayrel**.

Tunisia and the Kingdom of Morocco have both adopted data protection legislation with an objective to expand their attractiveness for the offshoring of services into their territory. Data Protection in Tunisia is governed by the Data Protection Act of 2004[1], and its implementation decrees of 2007[2]. In 2008, a report of the Moroccan Ministry of Economy pointed out that the low volume of relocation of banking and insurance services to Morocco was due partially to a lack of protection of personal data transferred to the Kingdom[3], and recommended the adoption of legislation on this subject, which followed in 2009[4].

The important political changes heralded by the Arab Spring in both countries (reorganisation of political structure of the State in Tunisia and constitutional revision in Morocco) and their future impacts on the development of privacy and data protection safeguards cannot be predicted yet. We will therefore limit this brief review to basic comments about the available legislation and current situation, whilst acknowledging that future changes may occur.

Tunisia: limited scope and lack of enforcement

The Tunisian Data Protection Act of 2004 affords protection to individuals[5] and applies both to automatic and non-automatic processing[6]. However, the Act leaves some issues unanswered or unaddressed with respect to its scope of application. Indeed, the Act only applies to physical persons or the representatives of the legal persons, processors and their agents having Tunisian nationality and their residence in Tunisia.[7] It seems to imply that foreign persons, companies and non-residents cannot be considered as "controllers", "processors" or "agents" in Tunisia, and therefore cannot be prevented from processing personal data on Tunisian territory. Nor does the Act attach any specific sanction to the violation of this provision. Such a regime obviously leads to a serious lack of legal certainty for international companies and is surprising considering the attractiveness of Tunisia as an offshore destination in the last decade.

Moreover, regarding the public sector, the Act includes a wide regime of derogations[8] following two criteria. The first one, the structural criterion, aims at exempting two explicitly mentioned categories of public persons: public authorities, local authorities and public establishments with administrative attributes on the one hand[9] and public health institutions and other public establishments without administrative attributes on the other hand[10]. The applicability of the derogation regime is further widened by an additional functional criterion, whereby both categories of public persons may avoid the operation of the Act when they process personal data in the course of specific functions. Where the first category of public persons acts "in the framework of public security or national defence, or to ensure legal prosecutions, or when said processing is necessary for the performance of their mission according to the relevant law in force" they are exempt. Likewise when the second category of public person acts "in the framework of the missions of which they are in charge of, by using the prerogatives of the public authorities according to the law in force". These provisions taken together seem to extend the derogatory regime potentially to all public sector activities.

> The Act demonstrates serious shortcomings. A major one relates to the absence of any right of access for individuals

General principles

Though the Act provides for the application of internationally recognised data protection principles, such as the purpose limitation principle[11], the data quality and proportionality principle[12], the security principle[13], some access and rectification rights[14], restrictions to onward transfers[15] and specific safeguards with respect to sensitive data[16], the Act demonstrates serious shortcomings. A major one relates to the absence of any right of access for individuals regarding processing carried out by all the public persons mentioned above[17]. Another one relates to the link established between the obligation to inform data subjects about the processing of information and the administrative obligations of the controller. Indeed, the obligation to inform data subjects about processing only applies in the cases where a declaration of the processing is required[18]. What is more, whenever an authorisation is required (e.g.: for the processing of data relating to health[19] or for video surveillance purposes[20]), the Act exempts the controller from its obligation of transparency[21].

Enforcement mechanisms

The *Instance Nationale de Protection des Données à Caractère Personnel* is composed of fifteen members

appointed by Decree by the President of the Republic for three-year terms[22] on the recommendation of the Minister of Justice and Human Rights. All the members but one are public officials. They come from all the three branches of power although the executive representation predominates since six members come from ministerial departments. The Act provides certain guarantees of independence to the DPA with respect to the private sector (duty of confidentiality[23], incompatibility regime[24]), but no comparable guarantee can be found towards the public sector.

The DPA (Data Protection Authority) is granted, according to the texts, some consultative, normative and inspection powers[25], which are traditional powers of any data protection regulatory authority. However the recent creation of the *Instance Nationale*[26] and the lack of available information regarding its actual activities[27] do not yet allow any conclusion concerning the effectiveness of the enforcement mechanisms in Tunisia. Finally, due to the immense political changes occurring in the country during 2011, it is fully understandable that data protection issues might not be considered as priorities.

Morocco: European inspired legislation in a Muslim State

The Data Protection Act of Morocco of 2009 demonstrates closer affiliation with the European directive 95/46, both in the wording and scope of application. It applies both to legal and natural persons, whether public or private. As in the Directive, the controller is understood to be the one who decides the purposes and means of the processing[28], without condition of residence or nationality. The Act affords protection to individuals, and excludes legal persons[29]. It covers automatic or partially automatic processing and manual processing when the personal data is intended to be in a data filing system.[30] Three matters are expressly excluded from the scope of the Act[31]:

1. The processing of personal data for exclusively domestic purposes;
2. Processing of personal data carried out in the interest of national defence and internal or external security of the State; and
3. Processing carried out for the purposes of prevention and repression of crime. The grounds for lawfulness of processing faithfully correspond to the ones laid down in the Directive 95/46.[32]

General principles

The Act provides for the most fundamental data protection principles, namely the purpose limitation principle and data quality and proportionality principles[33], the obligation of information[34], restrictions to onward transfers[35], direct marketing[36] and automated individual decisions[37], security principle[38] and rights of access, rectification and opposition[39] in certain cases to individual data subjects. Additional safeguards in case of processing of sensitive data are also laid down[40]. As in Tunisia[41], data concerning sex life are not considered as sensitive, though the definition of "sensitive data" follows closely the European one[42]. This can be explained by the Muslim character of the Moroccan State[43], where Islam is the State religion.[44] It is therefore perhaps surprising that the Legislator has recognised "philosophical and religious beliefs" as sensitive data, while the processing of this type of data is occurring regularly in a variety of situations in Morocco.[45] This inclusion must nevertheless be considered as coherent, since it can be invoked to restrict or prevent the collection and processing of a series of data that beyond the religious affiliation of a data subject, can indubitably be considered as sensitive.[46] In this context, the inclusion of philosophical and religious beliefs in the list of sensitive data for which processing must be submitted for prior authorisation by the National Data Protection Authority can be considered as a potential consolidation of liberties in the Kingdom.

Enforcement mechanisms

The *Commission nationale de contrôle de la protection des données à caractère personnel*[47] – the DPA – officially started to function on 2 September 2010. Its President, currently Said Ihrai, rector and professor of the faculty of law of Rabat, has been nominated by the King as well as its other six members (two of them on proposal by the prime Minister, two of them on proposal by the President of the "Chamber of Representatives" and two of them on proposal by the President of the "Chamber of Council")[48]. It is provided that the DPA shall be assisted by a General Secretary and provided with the necessary resources to carry out its tasks.

Though the independence of the DPA is not directly asserted in the Act, some guarantees can be derived from the following elements: the incompatibility regime according to which no member shall work, or have worked in the last five years, as an administrator or as a manager of a company specialised in the field of the processing of personal data[49]; the guarantee that when the DPA deliberates about an issue involving a public administration, members of the DPA coming from the government shall only have a consultative vote[50]; and the provision according to which members of the DPA shall be recruited both from the public and private sector and shall be known for their impartiality, expertise and competence[51].

The Data Protection Act has put in place a complaint mechanism[52]. However, sanctions have to be decided by the judiciary. In practice, at the end of an investigation, the DPA is requested to transmit to the Chief Prosecutor an official report indicating the infringements to the Data Protection Act. The Chief Prosecutor is then free to decide whether to institute legal proceedings which might lead to the adoption of sanctions.

Following its nomination and as provided in the Act, the DPA adopted its own internal regulation[53] and started its work. Though no official activity report has been drafted and published yet, the President asserts that the DPA has already been consulted by the government on specific cases and has dealt with its first complaints[54]. Moreover, the Commission has recently been accredited as a Data Protection Authority at the 33rd International Conference of Data Protection and Privacy Commissioners in Mexico City, November 2011.

Conclusion

While the Tunisian data protection regime shows major deficiencies with respect to the public sector, the Moroccan system seems more comprehensive and intended to address both public

and private processing activities. The new Moroccan DPA demonstrates a certain voluntarism in the taking of its functions. The lack of information concerning the Tunisian DPA activities does not yet allow proper assessment of its effectiveness in interpreting or enforcing the Act. Surely, the tremendous changes occurring in both countries may lead in future to substantial modifications to their current data protection regimes.

AUTHOR

Claire Gayrel, researcher, Centre de Recherche Informatique et Droit (CRID), Facultés Universitaires Notre-Dame de la Paix (FUNDP), Namur, Belgium.
Email: claire.gayrel@fundp.ac.be

AUTHOR

1. Tunisian Data Protection Act n°2004-63 of 27 July 2004
2. Implementation Decrees n°2007-3003 and n°2007-30004 of 27 November 2007 respectively relating to the functioning of the *Instance Nationale de Protection des Données à Caractère Personnel* and Implementation and to the condition of notification and authorisation and procedures for the processing of personal data
3. Report of the Ministry for economic affairs and finance of Morocco, *Délocalisation des activités de services au Maroc, Etat des lieux et opportunités*, june 2008, p. 15 www.finances.gov.ma/esp_doc/util/file.jsp?iddoc=2478
4. Moroccan Data Protection Act n°09-08 of 18 February 2009
5. See the definition of "personal data" in article 4 of the Act
6. Article 2 of the Tunisian Act
7. Article 22 of the Tunisian Act
8. Chapter V of the Tunisian Act
9. Article 53, §1 of the Tunisian Act
10. Article 53, §2 of the Tunisian Act
11. Articles 11 and 17 of the Tunisian Act
12. Articles 11 and 21 of the Tunisian Act
13. Articles 18 and 19 of the Tunisian Act
14. Sub-section III of the Tunisian Act
15. Article 51 and 52 of the Tunisian Act
16. Article 14 of the Tunisian Act
17. Article 56 of the Tunisian Act
18. Derives from the reading of article 31 and 7 of the Tunisian Act
19. See article 14 and 15 of the Tunisian Act
20. Article 69 of the Tunisian Act
21. Derives from Articles 31 and 8 of the Tunisian Act
22. Article 78 of the Tunisian Act and article 2 of the Implementation Decree relating to the DPA
23. Article 80 of the Tunisian Act
24. Article 79 of the Tunisian Act
25. Articles 76 and 77 of the Tunisian Act
26. The DPA held its first meeting on the 30th April 2009
27. www.inpdp.nat.tn/version-arabe/portail.html
28. See the definition of the "responsable du traitement", article 1 §5 of the Moroccan Act
29. See the definition of the concept of personal data, article 3 §1 of the Moroccan Act
30. Article 2, §1 of the Moroccan Act
31. Article 2, §4 of the Moroccan Act
32. Article 4 of the Moroccan Act
33. Article 3 of the Moroccan Act
34. Article 5 of the Moroccan Act
35. Article 43 of the Moroccan Act
36. Articles 9 and 10 of the Moroccan Act
37. Article 11 of the Moroccan Act
38. Article 23 of the Moroccan Act
39. Articles 7, 8 and 9 of the Moroccan Act
40. Article 21 of the Moroccan Act
41. See article 14 of the Tunisian Act which prohibits, as a rule, the processing of "personal data directly or indirectly relating to the ethnic or genetic origin, religious beliefs, political and philosophical opinions, trade-union memberships and health"
42. See the definition of "sensitive data" of article 1, §3 of the Moroccan Act : "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the data concerning health, including genetic data"
43. Preamble of the Constitution of 1 July 2011
44. Article 3 of the Constitution. Homosexual conducts and any sexual relationships outside the scope of marriage are actually sanctioned by criminal law (article 489 and 490 of the Criminal Code)
45. See for instance the Moudawana (Family Code) restricting marriage between Muslims and non Muslims
46. e.g.: "drink alcohol" or not, "frequent mosques" or not, "say one's prayers" or not et cetera…
47. Established under article 27 of the Moroccan Act
48. Article 2 of the Moroccan Implementation Decree
49. Article 35, §1 and 2 of the Moroccan Act
50. Article 38 of the Moroccan Act
51. Article 3 of the Moroccan Implementation Decree
52. Article 28 of the Moroccan Act
53. Decision of the Prime Minister n°3-33-11 approving the Commission's internal regulation of 28 march 2011 (23 rabii II 1432)
54. Interview with Saïd Ihrai, President of the DPA, 11 July 2011, *L'économiste*, www.leconomiste.com/print/885090

Mexico: DP regulations enter into force

The regulations of Mexico's Federal Law for the Protection of Personal Data entered into force on 22 December 2011 (*PL&B International* April 2011, p.26 and *PL&B International* September 2011, pp.7-8). The regulations deal with data subjects' rights, security and breach notification provisions, cloud computing, consent and notice requirements, and data transfers.

Data subjects can exercise their rights from January 2012. With regard to cloud computing, Article 52 of the regulations rules that cloud providers must comply with the DP law and the regulations, and clearly inform the data controller of any subcontracting.

"Therefore, the data controllers will be the ones with the de facto power to make the cloud providers comply with the provisions of the Regulations, by having the obligation to only hire cloud services which comply with the same", said Adolfo Athié at Basham, Ringe y Correa, S.C. in Mexico.

According to Basham, Ringe y Correa security measures to protect personal data held by private parties are required to be implemented within eighteen months following the effective date of the Regulations, and self-regulation arrangements may be implemented by private parties.

• *The regulations are at http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011 (in Spanish). Read more about this topic in the April issue of Privacy Laws & Business International Report.*